Преамбула: Техническое описание лабораторной инфраструктуры и общие требования к реализации.

В случае, если в тексте задания не указано иное, все пользовательские учетные записи должны иметь пароль P@ssw0rd.

Все проверки работы клиентских технологий (сайтов, клиентских VPN подключений и т.п.) будут выполняться из под пользователя user соответствующих клиентских машин.

При выполнении настоящего задания всегда нужно руководствоваться правилом наименьших привилегий.

Обратите внимание, что провайдерская адресация 100.64.0.0/10 относится к серому (частотному) диапазону адресов, что может потребовать дополнительных настроек на граничных сетевых устройствах межсетевого экранирования. Однако, в терминологии задания, сеть 100.64.0.0/10 относится к внешним (“белым”) сетям, наряду с “белыми” сетями из реального интернета.

Знак * (звёздочка, астериск) в задании является подстановочным знаком заменяет произвольную последовательность символов от начала строки или пробельного символа до другого пробельного символа или конца строки. К примеру, при указании на устройство FW* имеются ввиду все устройства в задании, название которых начинается с FW, например FW1, FW-MSK, FWabc и т.п., а при указании сетей *MSK имеются в виду все сети в задании, название которых заканчивается на MSK, например LAN1-MSK, SRV-MSK, dmzMSK и т.п.

Операционная система Traffic inspector next generation в интерфейсе при названии некоторых объектов не допускает использование символа “-”, в таком случае его можно заменять на знак “_”, но только там, где указать “-” невозможно.

В инфраструктуре функционирует DNS-провайдер (расположенный на ВМ ISP), его интерфейс доступен по адресу http://ns.ext/.

При настройке FreeIPA FQDN в обязательном порядке требуется указывать в нижнем регистре.

Согласно политике безопасности организации на устройствах с ОС Astra Linux и RedOS, допускается использование только официальных репозиториев. Данное правило не распространяется на внешних клиентов организации.

Предыстория:

После грандиозного успеха на Дальнем востоке, руководство отправило Вашу рабочую группу на помощь дружественной Организации в северо-западный

федеральный округ. Итак, перед Вами инфраструктура ООО СевЗапИгрКорп (далее - Организация), которая также занимается хостингом игровых серверов. Отличительной особеностью СевЗапИгрКорп является ориентированность на отечественный рынок и руководство организации хочет достичь максимально возможного уровня использования отечественных аппаратных и программных решений. На текущий момент в организации имеется два офиса, в городах Санкт-Петербург (внутреннее обозначение SPB) и Великий Новгород (NVR) а также виртуальный сервер в интернете с кодовым названием VDS. Все данное оборудование в филиалах только что распаковано, операционные системы предустановлены, дополнительную информацию о предустановленном ПО можно найти в разделах предоставленного вам для работы технического задания. Для широкополосного доступа к сети Интернет, компанией заключены договора с провайдерами интернета для обоих филиалов с предоставлением “белых” ip-адресов *(подробнее про сети провайдеров в разделе “Техническое описание лабораторной инфраструктуры и общие требования к реализации”). Также, у нас есть пара постоянных клиентов в городах Москва и Мурманск, которые с радостью предоставят нам свои компьютеры ClientMSK и ClientMRM для тестирования удаленного доступа к великолепным сервисам нашей компании.

Задания:

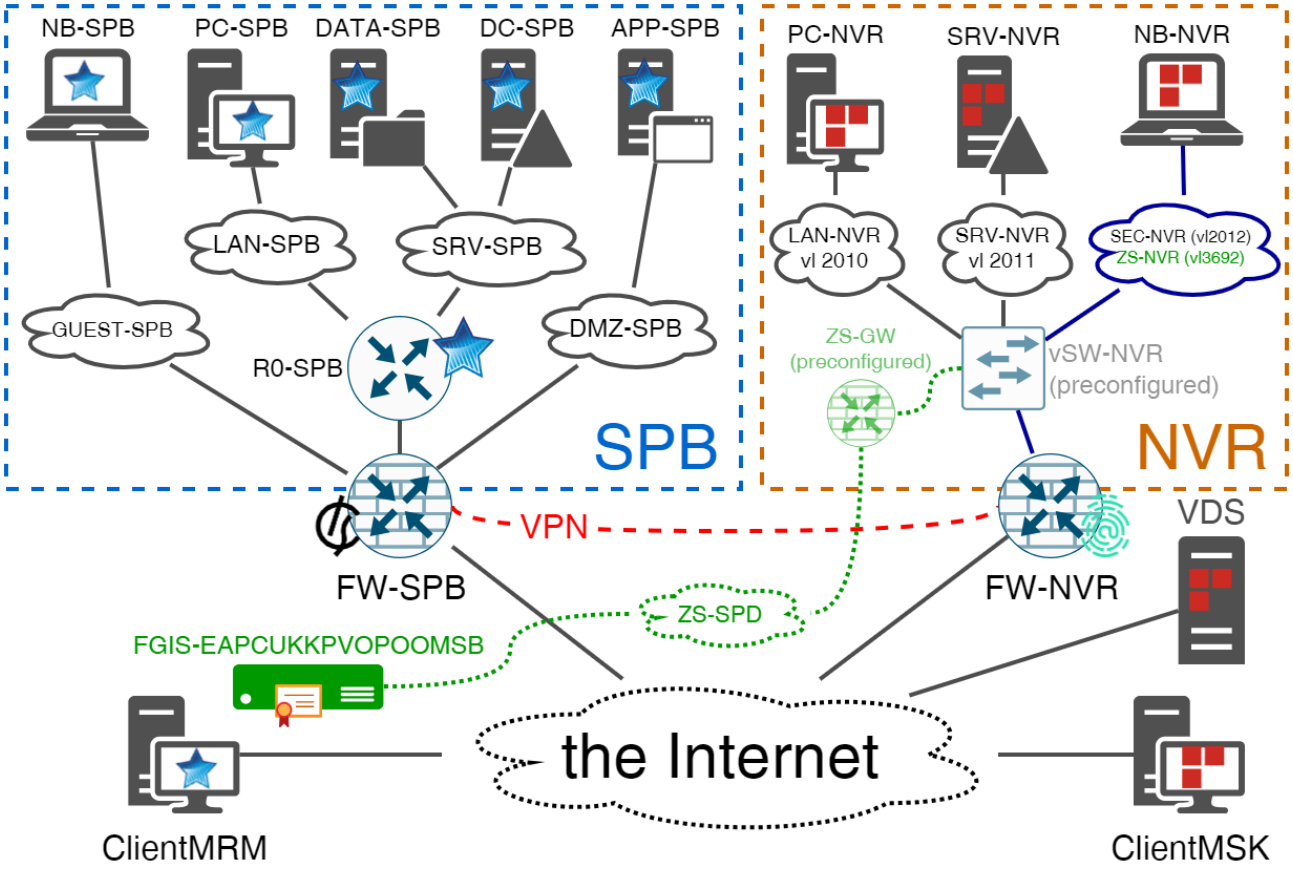
Схема адресации локальных сетей в задании разрабатывается участниками, однако требуется придерживаться следующих условий:

1. Для локальных сетей используется только приватная адресация из стандартных приватных диапазонов.
2. Все сети, соединяющие два маршрутизатора, включая сети туннелей site-to-site должны иметь маску сети /30.
3. Все остальные локальные сети, включая клиентские VPN-сети, должны иметь адресацию с маской /24. При этом шлюзом по умолчанию в таких сетях должен быть первый или последний адрес в сети, после принятия решения по адресации шлюзов по умолчанию, используйте аналогичные (только первые или только последние) адреса для шлюзов во всей инфраструктуре.
4. Все адреса loopback на маршрутизаторах должны иметь индивидуальную маску /32, но при этом быть из одного общего диапазона /24.

Схема IP-адресации и схема подключений.

Сеть	Устройство	Адрес/Маска	Шлюз
INTERNET	FW-SPB	100.67.32.80/26	ISP – первый адрес в сети
	FW-NVR	100.127.90.57/27	ISP – первый адрес в сети
	VDS	100.99.90.101/28	ISP – первый адрес в сети
	ClientMSK	100.108.128.45/28	ISP – первый адрес в сети
	ClientMRM	100.119.127.130/29	ISP – первый адрес в сети
	DNS-сервер	100.100.100.100	
	NTP-сервер	100.101.102.103	
ZS-SPD	Сеть ZS-SPD	172.24.0.0/14	
	FGIS-EAPCUKKP VOPOOMSB	172.26.146.157	
	ZS-GW	-	
FW-R0-SPB	FW-SPB	STATIC	
	R0-SPB	STATIC	FW-SPB
GUEST-SPB	FW-SPB	STATIC	
	NB-SPB	DHCP	FW-SPB
LAN-SPB	R0-SPB	STATIC	
	PC-SPB	DHCP	R0-SPB
SRV-SPB	R0-SPB	STATIC	
	DATA-SPB	STATIC	R0-SPB
	DC-SPB	STATIC	R0-SPB
DMZ-SPB	FW-SPB	STATIC	
	APP-SPB	STATIC	FW-SPB
LAN-NVR	FW-NVR	STATIC	

	PC-NVR	DHCP	FW-NVR
SRV-NVR	FW-NVR	STATIC	
	SRV-NVR	STATIC	FW-NVR
SEC-NVR	FW-NVR	STATIC	
	NB-NVR	DHCP	FW-NVR
ZS-NVR	ZS-GW	172.25.159.33/27	
	NB-NVR	STATIC	ZS-GW



Операционные системы:

VM	OS	GUI	Locale
FW-SPB	Интернет Контроль Сервер 10.2.2	-	ru_RU, en_US

R0-SPB	Astra Linux CE 2.12.46.6	-	ru_RU, en_US
NB-SPB	Astra Linux CE 2.12.46.6	FLY	ru_RU, en_US
PC-SPB	Astra Linux CE 2.12.46.6	FLY	ru_RU, en_US
DATA-SPB	Astra Linux CE 2.12.46.6	-	ru_RU, en_US
DC-SPB	Astra Linux CE 2.12.46.6	-	ru_RU, en_US
APP-SPB	Astra Linux CE 2.12.46.6	-	ru_RU, en_US
FW-NVR	Traffic inspector next generation 3.0.2.923	-	ru_RU, en_US
PC-NVR	RedOS 7.3.3	MATE	ru_RU, en_US
SRV-NVR	RedOS 7.3.3	-	ru_RU, en_US
NB-NVR	RedOS 7.3.3	MATE	ru_RU, en_US
VDS	RedOS 7.3.3	-	ru_RU, en_US
ClientMRM	Astra Linux CE 2.12.46.6	FLY	ru_RU, en_US
ClientMSK	RedOS 7.3.3	MATE	ru_RU, en_US

ЗАДАНИЕ первого дня

1. Настройте IPv4-адреса согласно схеме адресации:
   1.1. Настройте адреса шлюза по умолчанию, где это требуется;
   1.2. На FW* настройте описания интерфейсов, согласно схеме сети
   1.3. Обеспечьте отсутствие IPv6 адресации на FW* на всех интерфейсах, исключение допускается только для loopback-интерфейсов.
2. Настройте интерфейсы loopback на всех FW* и R*.
3. Настройте имена всех устройств согласно топологии.
4. Все устройства должны иметь доступ в интернет, если в задании явно не указано иного.
5. Настройте маршрутизацию, так, чтобы была обеспечена сетевая связность между всеми локальными сетями организации.

5.1. Маршрутизация, согласно политике безопасности организации, не является средством обеспечения безопасности и подразумевает наличие связности между всеми сетями Организации. Для разграничения доступа между сетями используется межсетевое экранирование, описанное в отдельных пунктах ТЗ

6. В филиале SPB разверните контроллер домена spb.jun.profi на базе FreeIPA с центром сертификации DogTag (далее - корпоративный центр сертификации) на сервере DC-SPB. При развертывании учтите, что это устройство будет выполнять функции DNS сервера в филиале SPB. Также, выполните следующие действия в развернутом домене:
   6.1. Создайте пользователей petr и alexandr, поместите их в группу profi-users
   6.2. Введите компьютер PC-SPB в домен, обеспечьте возможность входа под всеми доменными учетными записями на данный ПК.
   6.3. Создайте правило, разрешающее доменному пользователю admin использовать sudo на всех компьютерах в домене без ограничения.
   6.4. Обеспечьте доменному пользователю admin, после успешной авторизации на компьютере PC-SPB, возможность заходить в интерфейс FreeIPA без использования пароля. Для аутентификации и авторизации используйте Kerberos.
   6.5. Обеспечьте автоматическое монтирование директории /mnt/netshare/ на PC-SPB посредством autofs с авторизацией Kerberos. Сервер данного сетевого расположения - DATA-SPB, файлы на сервере располагаются в директории /opt/netshare/
7. Настройте инфраструктуру разрешения имен в филиалах следующим образом:
   7.1. DNS-сервер в филиале NVR располагается на FW-NVR.
   7.2. DNS-сервер в филиале SPB располагается на DC-SPB и интегрирован с доменом FreeIPA.
   7.3. Все устройства в локальных сетях должны обращаться с DNS запросами к DNS-серверам соответствующих филиалов
   7.4. Указанные DNS-сервера должны выполнять пересылку DNS запросов от локальных клиентов на DNS сервер провайдера, указанный в Схеме IP-адресации.
   7.5. Client* и VDS должны обращаться с DNS запросами на сервер провайдера, указанный в Схеме IP-адресации.
   7.6. Настройте для всех устройств филиалов в Санкт-Петербурге и Новгороде доменные имена в зонах spb.jun.profi и nvr.jun.profi соответственно.

7.7. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру dc-spb.spb.jun.profi или pc-nvr.nvr.jun.profi

7.8. В рамках каждого филиала короткие имена должны автоматически дополняться доменным именем соответствующего филиала

7.9. Создайте обратную зону(ы) DNS в доменном DNS-сервере DC-SPB, чтобы все ip-адреса в филиале SPB, расшифровывались в соответствующие им DNS-имена.

8. Настройте DHCP-сервера:
   8.1. на DC-SPB для клиентов сети LAN-SPB,
   8.2. на FW-SPB для клиентов сети GUEST-SPB,
   8.3. на SRV-NVR для клиентов сетей LAN-NVR и SEC-NVR.
   8.4. DHCP-сервер должен передавать клиентам все необходимые опции для работы в сети и взаимодействия с другими устройствами и сетями по IP и DNS именам.
   8.5. Выдаваемый диапазон адресов должен оставлять свободными ровно 10 адресов в начале сети, зарезервированных для дальнейшего использования, все остальные адреса должны предназначаться для выдачи клиентам по DHCP.
   8.6. Настройте необходимые параметры на промежуточных устройствах для получения адресной информации от соответствующих серверов.
9. Настройте синхронизацию времени
   9.1. Сервер точного времени в филиале SPB располагается на DC-SPB.
   9.2. Сервер точного времени в филиале NVR располагается на FW-NVR.
   9.3. Все устройства в локальных сетях должны использовать указанные сервера.
   9.4. Все сервера и клиенты, которые поддерживают Chrony должны использовать данную реализацию протокола. На устройствах, которые не поддерживают Chrony допускается использовать стандартный NTP.
   9.5. Указанные сервера времени, а также сервера и клиенты во внешних сетях должны синхронизировать свое время с NTP сервером по адресу 100.101.102.103.
   9.6. Все устройства организации должны функционировать в московском часовом поясе, при необходимости сделайте соответствующие настройки.

10. Обеспечьте авторизацию пользователей и межсетевое экранирование в сетях филиала SPB посредством функционала ПО, установленного на FW-SPB.
    10.1. В сети GUEST-SPB обеспечьте авторизацию пользователей через прокси
        10.1.1. Для авторизации используйте локального пользователя FW-SPB с именем guest-spb.
        10.1.2. Доступ к сетевым ресурсам должен появляться только после авторизации.
        10.1.3. Пользователи данной сети должны иметь доступ в интернет и не иметь доступа к локальным ресурсам, кроме необходимых для выполнения задания.
    10.2. В сети LAN-SPB обеспечьте авторизацию пользователей через captive portal. Для удобства сделайте на рабочем столе ярлык, который открывает страницу авторизации Captive Portal
    10.3. Обеспечьте возможность пользователям доменной группы profi-users авторизовываться в сетях филиала SPB со своими доменными учетными записями.
    10.4. Обеспечьте авторизацию всех серверов в филиале SPB по IP-адресам с автоматической связкой с mac-адресами при первой авторизации.
    10.5. Настройте правила межсетевого экранирования для сети DMZ-SPB:
        10.5.1. Устройства в сетях DMZ-* не должны иметь возможности инициировать соединения к клиентам в приватных сетях организации, при этом входящие соединения из всех остальных локальных сетей в сети DMZ-* должны быть разрешены.
        10.5.2. Устройства в сетях DMZ-* не должны иметь доступа к интернету, за исключением подключенных репозиториев ОС для установки и обновления пакетов и полного IPv4 доступа к серверу VDS.
        10.5.3. При необходимости, допускается возможность открывать конкретные дополнительные порты, необходимые для выполнения задания.
11. Настройте защищенный VPN-туннель FW-SPB<=>FW-NVR со следующими параметрами:
    11.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
    11.2. Используйте современные надежные протоколы шифрования AES, SHA-2 или ChaCha20.

11.3. Не допускается использование протоколов шифрования и аутентификации с длиной ключа/хеша менее 256 бит.

11.4. Настройте маршрутизацию, NAT и межсетевой экран таким образом, чтобы трафик для другого офиса не натировался и не блокировался.

12. Обеспечьте функционирование защищенного автоматизированного рабочего места (далее АРМ) на NB-NVR

12.1. Вход на АРМ должен быть доступен только под пользователем secure-user, иные пользователи должны быть заблокированы.

12.2. Пользователь secure-user должен иметь доступ к выполнению команд от имени суперадминистратора с проверкой пароля. При этом локальный вход под суперадминистратора должен быть запрещен.

12.3. К АРМ подключено два сетевых сегмента. Подключение осуществляется одним сетевым кабелем, а разделение сегментов осуществляется с помощью VLAN. Весь трафик тегирован.

12.4. Сеть ZS-NVR является защищенным сегментом, предназначенным для связи с ресурсами в закрытом сегменте сети передачи данных ZS-SPD. В ней имеется свой шлюз, который должен быть обязательно использован для доступа к ресурсам сети ZS-SPD. Направление трафика к ресурсам ZS-SPD любыми другими каналами строго запрещено.

12.5. Сеть SEC-NVR является локальным сегментом и предназначена для доступа к локальным ресурсам (только тем, которые необходимы для выполнения других пунктов задания) и разрешенным ресурсам в сети Интернет. Список разрешенных интернет-ресурсов:

12.5.1. Веб-сервисы VDS на стандартных портах

12.5.2. Официальные сайты операционных систем используемых в филиале NVR

12.5.3. Официальный сайт чемпионатного движения “Профессионалы”

13. Обеспечьте пользователю АРМ доступ к Системе ФГИС-ЭАПЦУККПВОПООМСБ в сегменте ZS-SPD

13.1.1. Вся известная о данной системе информация отражена в схемах и таблицах данного задания.

13.1.2. Требуется обеспечить доверие АРМ сертификату сайта данной информационной системы, используя корректную цепочку доверия.

13.1.3. Для обеспечения быстрого доступа к ФГИС-ЭАПЦУККПВОПООМСБ создайте ярлык на рабочем столе и добавьте сайт в закладки.

13.1.4. Заполните необходимые данные в ФГИС-ЭАПЦУККПВОПООМСБ в соответствии с расположенной в ней инструкцией.

ЗАДАНИЕ второго дня

1. Обеспечьте подключение клиента ClientMRM к серверу VPN на FW-SPB.
    1.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
    1.2. Используйте современные надежные протоколы шифрования AES, SHA-2 или ChaCha20.
    1.3. Клиент должен иметь доступ к серверам в сети SRV-SPB и DMZ-SPB.
    1.4. Соединение должно автоматически устанавливаться при включении компьютера или входе под пользователем user.
2. На сервере APP-SPB должен быть развернут WEB-сервер корпоративного портала организации:
    2.1. При развертывании корпоративного портала не используйте технологии контейнеризации
    2.2. Файлы сайта должны располагаться в директории /var/www/portal
    2.3. Сайт должен открываться по адресу corp.jun.profi
    2.4. Обращение к сайту из внутренних сетей организации должно происходить только по внутренним каналам связи, однако сайт должен также быть доступен и внешним клиентам по тому же адресу.
    2.5. Для работоспособности портала из внешнего мира, передайте необходимые настройки хостинг-провайдеру.
    2.6. Для портала разверните на веб-сервере CMS Wordpress актуальной стабильной версии. При необходимости, установите дополнительные программные компоненты на сервер.
    2.7. Сайт должен функционировать по протоколу HTTPS. При обращении по протоколу HTTP должен происходить автоматический редирект на HTTPS.
    2.8. WEB-сервер должен иметь сертификат, подписанный корпоративным центром сертификации
    2.9. Сайт должен открываться с PC-SPB и NB-NVR без ошибок и предупреждений.
    2.10. При обращении к серверу по ip-адресу или любому другому DNS-имени, кроме адреса корп.портала, сервер должен выдавать ошибку 404.
3. Обеспечьте подключение удаленного сотрудника с компьютера ClientMSK к корпоративному порталу https://corp.jun.profi следующим образом:

3.1. посредством VPN-подключения, когда оно активно.
3.2. посредством доступа по внешнему адресу, когда vpn-соединение неактивно.
3.3. Открытие портала не должно вызывать ошибок и предупреждений безопасности.

4. Настройте почтовый сервер на FW-SPB
   4.1. Обеспечьте автоматическое создание почтовых ящиков для пользователей из группы profi-users в имеющемся домене FreeIPA
   4.2. Обеспечьте возможность входа в почтовые ящики с компьютеров PC-SPB, PC-NVR, и ClientMRM
   4.3. Обращение к почтовому серверу из внутренних сетей организации должно происходить только по внутренним каналам связи, однако он должен также быть доступен и внешним клиентам.
   4.4. Обеспечьте возможность входа в почтовые ящики с ClientMSK посредством VPN-соединения.
   4.5. Для подключения к почтовому серверу используете любой бесплатный/“свободный”/“открытый” почтовый клиент с графическим окружением. Для удобства пользователя создайте на рабочем столе ярлык на установленный почтовый клиент.
5. Обеспечьте веб-интерфейс FW-SPB сертификатом HTTPS, подписанным корпоративным центром сертификации, обеспечивающим доверенное соединение при обращении к FW-SPB по полному и сокращенному DNS-имени и IP-адресу с PC-SPB.
6. Обеспечьте возможность подключения к FW-NVR под пользователем admin:
   6.1. посредством веб-интерфейса с полным доступом к настройкам;
   6.2. посредством протокола SSH с доступом к выполнению команд через sudo;
   6.3. при подключении с компьютера PC-NVR авторизация SSH должна осуществляться по ключу без необходимости ввода пароля.
7. Настроить удаленный доступ к VDS и R0-SPB по SSH
   7.1. На сервере VDS сервис SSH должен функционировать на порте 2202
   7.2. Устройство PC-SPB при входе под пользователем user должно иметь доступ к VDS под пользователем user с использованием SSH ключей, без необходимости ввода пароля.

7.3. Пользователь user на VDS должен иметь возможность выполнять команды через sudo без ввода пароля.
7.4. Подключение к VDS с PC-SPB должно осуществляться командой “ssh VDS” без дополнительных параметров.
7.5. Устройство PC-SPB при входе под пользователем user должно иметь доступ к R0-SPB под пользователем user с использованием SSH ключей, без необходимости ввода пароля.

8. Для хранения важных данных в сервер VDS установлено два дополнительных диска. Объедините их в RAID1 используя технологию md raid. На полученном резервированном носителе создайте файловую систему XFS и подключите раздел по пути /opt/mc/data/ для дальнейшего использования.
9. На VDS разверните сервер Minecraft со следующими параметрами:
    9.1. Имя сервера: Jun Profi
    9.2. Ограничение кол-ва игроков: 12
    9.3. Порт: по умолчанию
    9.4. Проверка аккаунтов пользователей: отключена
    9.5. Сервер должен быть запущен в виде контейнера Docker
    9.6. Данные сервера должны храниться по пути /opt/mc/data/
    9.7. Контейнер должен автоматически запускаться после перезагрузки компьютера.
10. Помогите постоянному клиенту из Омска подготовить рабочее место ClientMSK:
    10.1. Установите tlauncher. Обязательно создайте ярлык установленного tlauncher на рабочем столе пользователя, чтобы ему было удобнее подключаться к Вашему серверу.
    10.2. Установите OBS последней стабильной версии посредством системы управления пакетами Flatpak. Обязательно создайте ярлык установленного OBS на рабочем столе пользователя, чтобы ему было удобнее запускать стрим игры на Вашем сервере.
11. На сервере SRV-NVR разверните сервер мониторинга со следующими параметрами:
    11.1. Сервер: Zabbix LTS
    11.2. Веб-интерфейс: на основе Nginx
        i. Основной адрес: mon.nvr.jun.profi
        ii. Порт веб-интерфейса: 80(HTTP), 443(HTTPS)
        iii. Автоматическая переадресация на безопасный протокол
        iv. Сертификат подписан корпоративным ЦС

11.3. База данных: PostgreSQL
11.4. Веб интерфейс БД: PgAdmin
    i. Порт PgAdmin: 8888
    ii. Подключите PgAdmin к созданному серверу БД с полным административным доступом под пользователем pgadm@jun.profi
11.5. Все сервисы должны быть запущены в виде контейнеров Docker
11.6. Все контейнеры должны автоматически запускаться после перезагрузки компьютера

12. Настройте развернутый сервис мониторинга следующем образом:
    12.1. Добавьте на сервер все сервера и сетевые устройства организации
    12.2. Обеспечьте сбор базовых показателей со всех подключенных устройств

ЗАДАНИЕ третьего дня

По результатам вашей успешной работы, руководство отправило вас на курсы повышения квалификации по теме “Поиск и устранение неисправностей в сетевых инфраструктурах малого и среднего бизнеса”. На время вашего отсутствия ваши обязанности временно исполнял студент-практикант. Качество его работы вызвало у руководства большие вопросы и теперь вам представляется уникальная возможность применить полученные знания на реальной практике.

В данном разделе вам будет предложено 15 заявок от пользователей в техническую поддержку, накопившиеся за определенное время. При этом, заведомо известно, что в какой-то момент все работало идеально, однако потом вышло из строя самостоятельно или было повреждено некорректными действиями пользователя или временного технического персонала.

Примеры возможных заявок:

1. Клиенты из сети LAN-SPB потеряли доступ в интернет
2. Компьютеры в филиале NVR не могут обращаться по именам к компьютерам в домене
3. Сотрудник за PC-NVR не может обратиться на DATA-SPB по внутреннему адресу
4. Minecraft на VDS не работает, хотя контейнер запущен.
5. На VDS было два пользователя: user1 и user2. Но при попытке зайти на машину, используя эти два логина ничего не получалось. Файлы и группы пользователей должны быть сохранены.
6. Сотрудник работающий из дома не может подключиться к серверам во внутренней инфраструктуре организации.
7. Корпоративный портал открывается с ошибкой сертификата.
8. Пользователь на NB-NVR не может обратиться к сайту ФГИС-ЭАПЦУККПВОПООМСБ по имеющемуся у него ярлыку
9. Пользователь petr на компьютере PC-SPB не может записывать файлы в примонтированную сетевую директорию
10. В интерфейсе системы мониторинга перестала появляться информация с сервера DC-SPB